In the Drawings

In response to the objections to the drawing in the Office Action (page 2), Applicants submit herewith four (4) Sheets of Replacement Drawings and four (4) Sheets of Annotated Drawings. As illustrated on the Annotated Sheets, the Replacement Sheets add the legend "Prior Art" to Figs. 1-4 as suggested in the Office Action.

The Replacement Drawings are in compliance with 37 C.F.R. 1.121(d) and 37 C.F.R. §1.84(c). Accordingly, Applicants respectfully request that the objections to the drawings be withdrawn.

REMARKS

In response to the Office Action mailed September 2, 2005, Applicants respectfully request reconsideration.

Claims 1-23 were previously pending in this application. By this amendment, Applicants amend claims 3, 11, 14, 18, and 20. As a result, claims 1-23 are pending for examination, of which claims 1, 3, 4, 6, 11, 13, 18, 20, and 22 are independent. No new matter has been added.

1. Claim 14 is Not a Duplicate of Claim 15

Claim 14 stands objected-to as being a duplicate of claim 15. However, claim 14 recites *inter alia*, "each of the plurality of small packets," whereas claim 15 recites, *inter alia*, "the IKE packet." Accordingly, claim 14 is not a duplicate of claim 15, and Applicants respectfully request that the objection of claim 14 be withdrawn.

2. Claims 1 and 2 Patentably Distinguish Over IPSEC in View of Kent

Claims 1 and 2 stand rejected under §103(a) as purportedly being unpatentable over the Minutes of IPSEC Working Group meeting found on http://www.ietf.org/proceedings/01dec/195/htm (IPSEC) in view of *Fragmentation Considered Harmful* by Christopher A. Kent and Jeffery C. Mogul, 8282 Computer Communication Review 25 (1995) (Kent). Applicants respectfully traverse this rejection.

2.1 Background

As is well known to those of skill in the art, protocols and technologies dealing with the communication of information between nodes of a communication network can be divided into several layers of a networking protocol framework, such as, for example, the seven layers of the Open System Interconnection (OSI) model. Although there is some debate as to which layers of the framework certain protocols and technologies belong, it is well-settled that the Internet Protocol (IP) resides at the network layer (i.e., layer 3) of the networking protocol framework, and that the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) reside at the transport layer (i.e., layer 4) of the networking protocol framework.

IP Security (IPsec) is a set of protocols developed by the Intranet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer. IPsec has been deployed widely to

implement Virtual Private Networks (VPNs). For IPsec to work, the sending and receiving devices must share a public key. The Internet Key Exchange (IKE) protocol is a key management protocol standard, which often is used in conjunction with the IPsec standard. IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

2.2 Discussion of IPSEC

The IPSEC Working Group is a work group of the ITEF charged with developing mechanisms to protect client protocols of IP, including developing a security protocol in the network layer to provide cryptographic security services that flexibly support combinations of authentication, integrity, access control and confidentiality. (Page 1). IPsec deals with a variety of issues relating to the above charter, including changes to IKE to support Network Address Translation (NAT) Firewall traversal. (Page 1)

IPSEC indicates that the testing of IPsec over NAT revealed some problems, including certificate fragmentation. (Page 3, last line – page 4, line 6). Possible approaches to avoid fragmentation were considered, including fragmenting packets at a layer of the networking protocol framework that is above the transport layer at which the User Datagram Protocol (UDP) protocol resides. (Page 4, lines 8-10).

2.3 Discussion of Kent

Kent is directed to fragmentation in the context of the IP protocol (Page 75, second column, first full paragraph). Kent provides an explanation of what is wrong with fragmentation (Section 2) and describes how to avoid fragmentation (Section 3).

The Office Action contends that "Kent discloses that it is advantageous to avoid fragmentation at the IP layer, by employing methods for IP layer fragmentation avoidance *at upper level protocol layers*." (emphasis added). However, not only does Kent not disclose IP layer fragmentation at upper level protocol layers, but it discloses the very opposite, that fragmentation should be performed at the IP datagram layer, i.e., the network layer (i.e., layer 3 or IP layer) of the networking protocol framework. Specifically, Kent discloses that "[f]ragmentation avoidance must be done at the right layer. It makes little sense to build redundant mechanisms into several layers if it is possible to do it once. This implies that *the*

right place for fragmentation avoidance is the layer common to all IP communication, the IP datagram layer itself." (Page 79, first column, third full paragraph; *emphasis added*).

2.4 The Combination of IPSEC and Kent is Improper

The combination of IPSEC and Kent is improper because, at the time of the invention, one skilled in the art would not have been motivated to combine IPSEC and Kent as indicated in the Office Action. The Office Action asserts that "it would have been obvious to one of ordinary skill in the art to employ the specific methods of Kent et al. for general packet fragmentation as well as methods for *fragmentation avoidance above the IP layer* with the general teachings of IPSEC for acquiring the fragmentation of IKE packets above the IP layer." (*emphasis added).* However, as discussed above, Kent does not disclose or suggest fragmentation avoidance above the IP layer, but rather, specifically indicates that fragmentation should be performed at the IP layer itself. Thus, one of skill in the art would not have been motivated to combine Kent and IPSEC as suggested in the Office Action.

2.5 Claim 1 Patentably Distinguishes Over the Combination of IPSEC and Kent

Even if it were proper to combine IPSEC and Kent (which it is not), claim 1 would patentably distinguish over such combination. Kent does not disclose or suggest all of the limitations of the method of transmitting IKE data packets across a network recited in claim 1, in particular, the step of "fragmenting the IKE packet into a plurality of smaller packets *when a response is not received.*" The Office Action contends that IPSEC teaches this limitation in Section 3.3. However, in contrast to determining when a response is not received, Kent discloses determining when fragmentation occurs, and further fragmenting a datagram in response to determining that a fragmentation has occurred. (Section 3.3, first and second paragraphs). All of the methods described in Sections 3.3.1 – 3.3.5 deal with detecting whether fragmentation occurs, not whether a response to a data packet was received. In fact, several of these methods involve fragmenting a datagram when a response of some sort **is received**, such as, for example, a "Time Exceeded" message (Section 3.3.3), a "Fragmentation Warning" message (Section 3.3.4), and a "Fragments Received" message (Section 3.3.5).

IPSEC fails to remedy these deficiencies of Kent. Accordingly, even if IPSEC and Kent were combined, the combination would not disclose or suggest a method for transmitting IKE

data packets across a network comprising, *inter alia*, fragmenting the IKE packet into a plurality of smaller data packets *when a response is not received.*

2.6 Conclusion Regarding Claims 1 and 2

In view of the foregoing, claim 1 patentably distinguishes over IPSEC in view of Kent. Accordingly, Applicants respectfully request that the rejection of claim 1 under §103(a) be withdrawn. Claim 2 depends from claim 1 and is patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claim 2 be withdrawn.

3. Claim 3 Patentably Distinguishes Over IPSEC

Claim 3 stands rejected under Section 102(a) as being anticipated by IPSEC. Applicants respectfully traverse this rejection.

Claim 3 as amended, recites:

> A network node that communicates with other network nodes according to the Internet Key Exchange (IKE) protocol comprising:
>
> a User Datagram Protocol (UDP) stack that is capable of generating UDP data packets for transmission over a network;
>
> an IKE protocol stack that generates IKE data packets that are subsequently processed by the UDP protocol stack; and
>
> a fragmenter module that intercepts IKE data packets prior to being processed by to the UDP protocol stack and splits the IKE data packets into a plurality of smaller data packets that may be subsequently formatted by the UDP protocol stack,
>
> **wherein, each of the plurality of smaller data packets includes a header formatted according to the IKE protocol.**

Claim 3 as amended patentably distinguishes over IPSEC because IPSEC does not disclose or suggest all of the limitations of the network node that communicates with other network nodes according to the IKE protocol recited in claim 3. In particular, IPSEC does not teach the limitation that each of the plurality of smaller data packets includes a header formatted according to the IKE protocol. IPSEC merely mentions that

fragmentation of a packet may occur above the transport layer at which UDP resides. However, IPSEC does not disclose or suggest including in the fragments a header formatted according to the IKE protocol. In fact, IPSEC is silent regarding any of the details of how the fragmentation of the data above the transport layer is performed.

In view of the foregoing, claim 3 as amended patentably distinguishes over IPSEC. Accordingly, Applicants respectfully request that the rejection of claim 3 under §102(a) be withdrawn.

4. Claims 4-5 Patentably Distinguish Over IPSEC in View of Kent

Claim 4 stands rejected under Section 4 as purportedly being unpatentable over IPSEC in view of Kent. Applicants respectfully traverses this rejection.

For reasons set forth in Section 2 above, the combination of IPSEC and Kent is improper. Further, even if the combination were proper (which it is not), the resulting system would not employ the method recited in claim 4.

Claim 4 recites:

> A method for fragmenting a data packet comprising the steps of:
> generating an **IKE data packet**;
> intercepting the **IKE data packet** before it is passed to a subsequent network protocol stack;
> determining a maximum size for fragments of an **IKE data packet**;
> dividing the **IKE data packet** into at least two smaller packets; and
> prepending a header to each smaller packet, wherein each header for each smaller packet includes an identifier that associates the smaller packet with its corresponding **IKE data packet**.

Neither IPSEC nor Kent disclose or suggest the concept of an IKE data packet. As noted above, IPSEC merely discloses that fragmentation of a data packet may occur at a layer above the transport layer of a networking protocol framework, but provides no description of how this fragmentation occurs. Nor does Kent disclose the concept of an IKE data packet. In contrast to the assertions of the Office Action (page 6, bottom), Kent

does not disclose or suggest generating an IKE data packet, intercepting an IKE data packet, determining a maximum size for fragments of an IKE data packet and dividing the IKE data packet into at least two smaller data packets. In contrast, Kent is only concerned with fragmentation of IP data packets. That is, Kent (Section 2.1) provides a description of fragmenting IP datagrams into packets at the networking layer (layer 3) only, and makes no suggestion of doing so at any other layer, as described above. Accordingly, even if it were proper to combine IPSEC and Kent, the resulting combination would not employ a method that uses IKE data packets in any fashion.

In view of the foregoing, claim 4 patentably distinguishes over IPSEC in view of Kent. Accordingly, Applicants respectfully request that the rejection of claim 4 under §103(a) be withdrawn. Claim 5 depends from claim 4 and is patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claim 5 be withdrawn.

5. Claims 6-10 Patentably Distinguish Over IPSEC in View of Kent

Claim 6 stands rejected under Section 103(a) as purportedly being unpatentable over IPSEC in view of Kent. Applicants respectfully traverses this rejection.

As set forth in Section 2 above, the combination of IPSEC is improper. Even if the combination was proper (which it is not), claim 6 patentably distinguishes over such combination.

Claim 6 recites:

> A method for receiving fragmented Internet Key Exchange (IKE) data packets comprising the steps of:
> receiving a plurality of fragments of an **IKE data packet** from a transmitting node, wherein each fragment includes an identifier that associates each fragment with an **IKE data packet**; and
> discarding all fragments that contain a first identifier if a predetermined number of fragments are received that contain a second identifier.

Claim 6 patentably distinguishes over IPSEC and Kent for reasons that should be clear from the discussions of Kent and IPSEC set forth in Section 4. The combination of

IPSEC and Kent would not disclose or suggest the method recited in claim 6, including, *inter alia*, the step of receiving a plurality of fragments of an **IKE data packet**. As noted above, neither IPSEC nor Kent discloses or suggests IKE data packets. Thus, the resulting combination would not employ a method that uses IKE data packets.

In view of the foregoing, claim 6 patentably distinguishes over IPSEC in view of Kent. Accordingly, Applicants respectfully request that the rejection of claim 6 under §103(a) be withdrawn. Claim 7-10 each depend from claim 6 and are patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejections of claims 7-10 be withdrawn.

6. Claims 11 and 12 Patentably Distinguish Over IPSEC in View of Kent

Claim 11 stands rejected under Section 103(a) as purportedly being unpatentable over IPSEC in view of Kent. Applicants respectfully traverse this rejection.

For the reasons set forth above in Section 2, the combination of IPSEC and Kent is improper. Further, even if the combination were proper (which it is not), claim 11 would patentably distinguish over such combination.

Claim 11 patentably distinguishes over the combination of IPSEC and Kent because such combination would not disclose or suggest all of the limitations of the system for transmitting IKE protocol data packets across a network recited in claim 11. In particular, the combination would not disclose the limitation of "means for fragmenting the IKE data packets into smaller data packets **when the IKE data packet was not successfully received at the receiver node**," as required by claim 11. As discussed in previous sections, neither IPSEC nor Kent disclose or suggest the concept of an IKE packet, nor generating one, attempting whether it was successfully received, or fragmenting one into smaller packets. Thus, no system resulting from the combination of these references would include means for performing any of these functions.

In view of the foregoing, claim 11 patentably distinguishes over IPsec in view of Kent. Accordingly, Applicants respectfully request that the rejection of claim 11 under §103(a) be withdrawn. Claim 12 depends from claim 11 and is patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claim 12 be withdrawn.

7. Claim 13 Patentably Distinguishes Over IPSEC in View of Kent.

Claim 13 stands rejected under §103(a) as purportedly being unpatentable over IPSEC in view of Kent. Applicants respectfully traverse this rejection.

As set forth in Section 2 above, the combination of IPSEC and Kent is improper. Further, even if the combination were proper, claim 13 patentably distinguishes over such combination.

Claim 13 patentably distinguishes over the combination of IPSEC and Kent because the combination does not teach or suggest all of the limitations of the method for transmitting data packets across a network recited in claim 13. In particular, neither teaches or suggests the concept of an IKE packet recited in claim 13, including generating and transmitting an IKE packet, determining whether a response to the IKE packet was received, nor fragmenting an IKE packet. Further, neither reference teaches or suggests the step of fragmenting the IKE packet into a plurality of smaller packets *when a response is not received.* As set forth above, Kent does not disclose fragmenting any type of packet into a plurality of smaller packets when a response is not received. Rather, Kent discloses fragmenting datagrams into IP packets (at the IP layer) in response to determining that previously transmitted packets were fragmented by other nodes along a communication path. Further, several of the methods employed by Kent in fragmenting packets involve doing so when a response of some sort is received from another node, not when a response is *not* received. Thus, no combination of IPSEC and Kent would employ a method that uses IKE packets and/or fragments a packet into a plurality of smaller packets when a response is *not* received.

In view of the foregoing, claim 13 patentably distinguishes over IPSEC in view of Kent. Accordingly, Applicants respectfully request the rejection of claim 13 under §103(a) be withdrawn. Claims 14-17 each depend from claim 13 and are patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejections of these claims be withdrawn.

8. Claims 18 and 19 Patentably Distinguish Over IPSEC in View of Kent.

Claims 18 and 19 stand rejected under Section 103(a) as purportedly being obvious over IPSEC in view of Kent. Applicants respectfully traverse this rejection.

The combination of IPSEC and Kent is improper for at least the reasons set forth above in Section 2. Further, even if the combination were proper (which it is not), claim 18 as amended patentably distinguishes over such combination.

Claim 18 as amended, recites:

> A method of arranging information for transmission across a network comprising the steps of:
>
> generating a data packet containing Internet Key Exchange (IKE) information; determining whether fragmentation of the data packet is necessary to successfully transmit the IKE information over a network; and
>
> fragmenting the data packet if necessary into a plurality of smaller packets that may be transmitted over a network,
>
> **wherein the steps of generating, determining and fragmenting are performed independently of performing any steps on the data packet corresponding to a transport layer protocol and/or a network layer protocol.**

Claim 18 patentably distinguishes over the combination of IPSEC and Kent because such combination does not teach or suggest all of the limitations of the method of arranging information for transmission across a network recited in claim 18. Specifically, the combination does not teach or suggest that the steps of generating, determining and fragmenting are performed independently of performing any steps on the data packet corresponding to a transport layer protocol and/or a network layer protocol, as required by claim 18. Rather, Kent discloses fragmenting and/or avoiding fragmentation of data packets using a network layer protocol (i.e., an IP protocol). Further, although IPSEC mentions fragmenting packets at a layer above transport layer of the networking protocol framework, IPSEC does not disclose or suggest determining whether fragmentation of a data packet is necessary to successfully transmit IKE information over a network. Accordingly, even if IPSEC and Kent were combined, the resulting combination would not teach or suggest performing the steps of generating, determining and

fragmenting independently of performing any steps corresponding to a transport layer protocol and/or a network layer protocol.

In view of the foregoing, claim 18 patentably distinguishes over IPSEC in view of Kent. Accordingly, applicants respectfully request that the rejection of claim 18 under §103(a) be withdrawn. Claim 19 depends from claim 18 and is patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claim 19 be withdrawn.

9. Claims 20 and 21 Patentably Distinguish Over IPSEC in View of Kent.

Claim 20 stands rejected under §103(a) as purportedly being unpatentable over IPSEC in view of Kent. Applicants respectfully traverse this rejection.

The combination of IPSEC and Kent is improper for at least the reasons set forth above in Section 2. Further, even if the combination were proper (which it is not), claim 20 patentably distinguishes over such combination.

Claim 20 as amended, recites:

> A method for resolving transmitting errors associated with transmitting Internet Key Exchange (IKE) packets via protocol stacks that implement the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), and/or the Internet Protocol (IP) comprising the steps of:
>
> generating a data packet containing IKE data;
>
> fragmenting the packet to a plurality of fragments using a code module that does not implement the TCP, UDP or IP protocols before the packet is processed by a code module that does implement the TCP, UDP or IP protocols, comprising **including an identifier that identifies the data packet in each packet fragment;** and
>
> transmitting the packet fragments over a network.

The combination of IPSEC and Kent does not teach or suggest all of the limitations of the method for resolving transmission errors recited in claim 20. Specifically, such combination does not teach or suggest the step of fragmenting the data packet into a plurality of fragments using a code module that does not implement the TCP, UDP or IP protocols before the packet is processed by a code module that does implement the TCP, UDP or IP protocols, comprising, *including an identifier that identifies the data packet in each packet fragment.* Kent only discloses generating and fragmenting packets using IP protocols. Although IPSEC discloses

fragmenting a packet at a layer above the transport layer at which UDP resides, IPSEC does not teach or suggest including an identifier in each packet fragment that identifies the data packet. In fact, IPSEC is silent regarding any of the implementation details associated with fragmenting a packet at a layer above the transport layer. Accordingly, even if IPSEC and Kent were combined, the resulting combination would not employ a method of resolving transmitting errors that comprises, *inter alia*, including an identifier that identifies the data packet in each *packet fragment*.

In view of the foregoing, claim 20 patentably distinguishes over IPSEC in view of Kent. Accordingly, applicants respectfully request that the rejection of claim 20 under §103(a) be withdrawn. Claim 21 depends from claim 20 and is patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claim 21 be withdrawn.

10. Claims 22 and 23 Patentably Distinguish Over IPSEC in View of Kent.

Claim 22 stands rejected under §103(a) as purportedly being unpatentable over IPSEC in view of Kent. Applicants respectfully traverse this rejection.

For the reasons set forth in Section 2 above, the combination of IPSEC and Kent is improper. Further, even if the combination were proper (which it is not), claim 22 would patentable distinguish over such combination.

The combination of IPSEC and Kent does not teach or suggest all of the limitations of the method for intelligently discarding data packets to efficiently manage resources recited in claim 22. Specifically, such combination does not teach or suggest the step of discarding at least certain of the received packets **when a predetermined number of out-of-order packets have been received**, as required by claim 22. The Office Action contends that Kent discloses this step in Section 2.1, paragraph 3 and in Section 2.4, paragraph 3. Applicants respectfully disagree. Section 2.1, paragraph 3 describes the Time to Live (TTL) field of an IP packet header and describes that a packet must be discarded if the TTL contains the value 0. Section 2.4, paragraph 3 describes that entire packets may have to be discarded during reassembly if there is not enough buffer space to accommodate multiple data packets simultaneously. Thus, Kent does not teach or suggest discarding received packets *when a predetermined number of out-of-order packets have been received.* IPSEC fails to remedy this deficiency of Kent. Accordingly even if IPSEC

and Kent were combined, neither would employ the discarding step recited in claim 22.

In view of the foregoing, claim 22 patentably distinguishes over IPSEC in view of Kent. Accordingly, Applicants respectfully request that the rejection of claim 22 under §103(a) be withdrawn. Claim 23 depends from claim 22 and is patentable for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claim 23 be withdrawn.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed, Applicants hereby requests the necessary one-month extension of time. Applicants enclose a check to cover the extension fee associated with this filing. If the amount is insufficient, the Commissioner is hereby authorized to charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,

Brian D. Swander et al., Applicants

By: _____

Daniel P. McLoughlin, Reg. No. 46,066
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000

Docket No.: M1103.70145US00
Date: January 3, 2006

METHOD AND APPARATUS FOR FRAGMENTING AND REASSEMBLING INTERNET KEY EXCHANGE DATA PACKETS
Applicant: Swander et al.
Serial No.: 10/056,889
Docket No.: M1103.70145US00
Figure 1
ANNOTATED SHEET SHOWING CHANGES

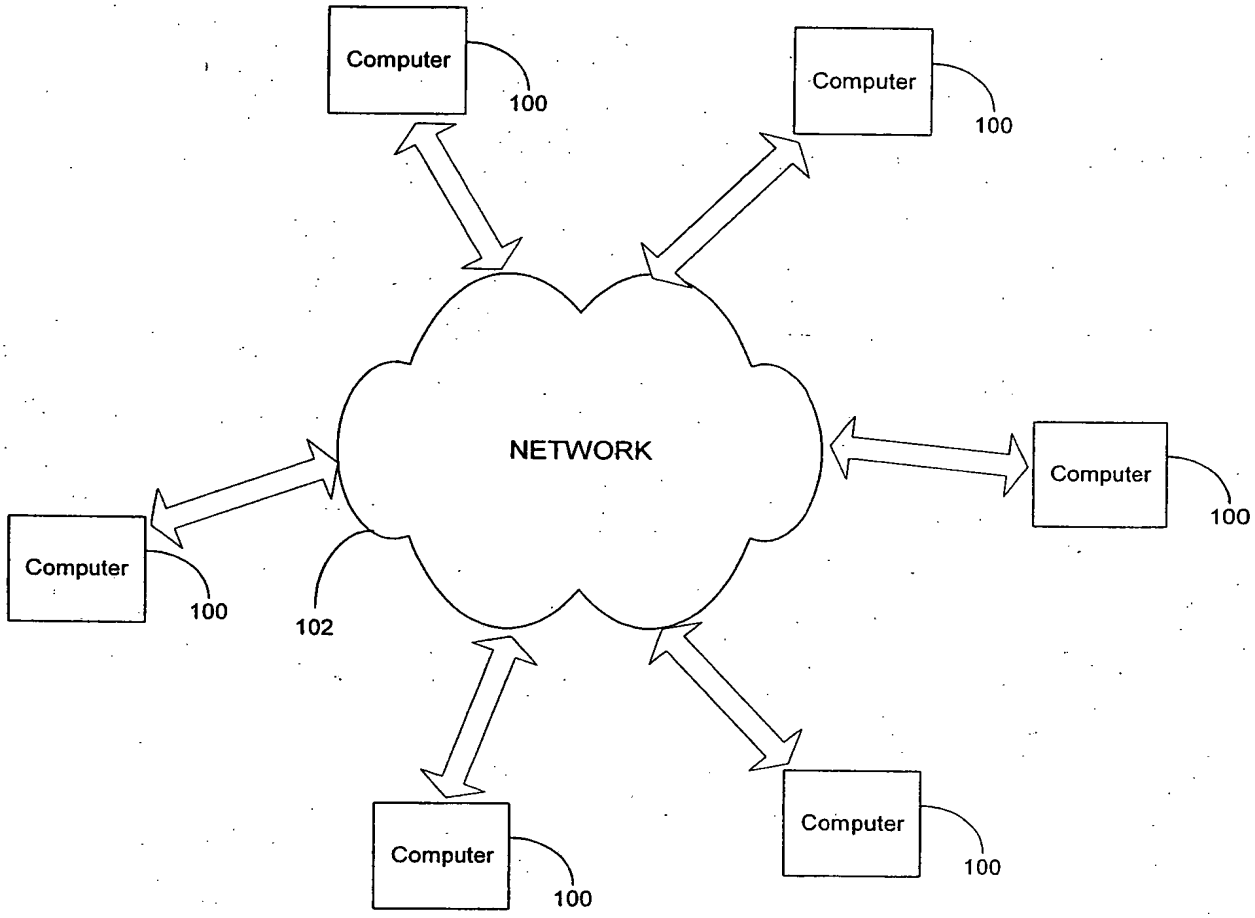

FIG. 1 (Prior Art)

METHOD AND APPARATUS FOR FRAGMENTING AND REASSEMBLING INTERNET KEY EXCHANGE DATA PACKETS
Applicant: Swander et al.
Serial No.: 10/056,889
Docket No.: M1103.70145US00
Figure 2
ANNOTATED SHEET SHOWING CHANGES

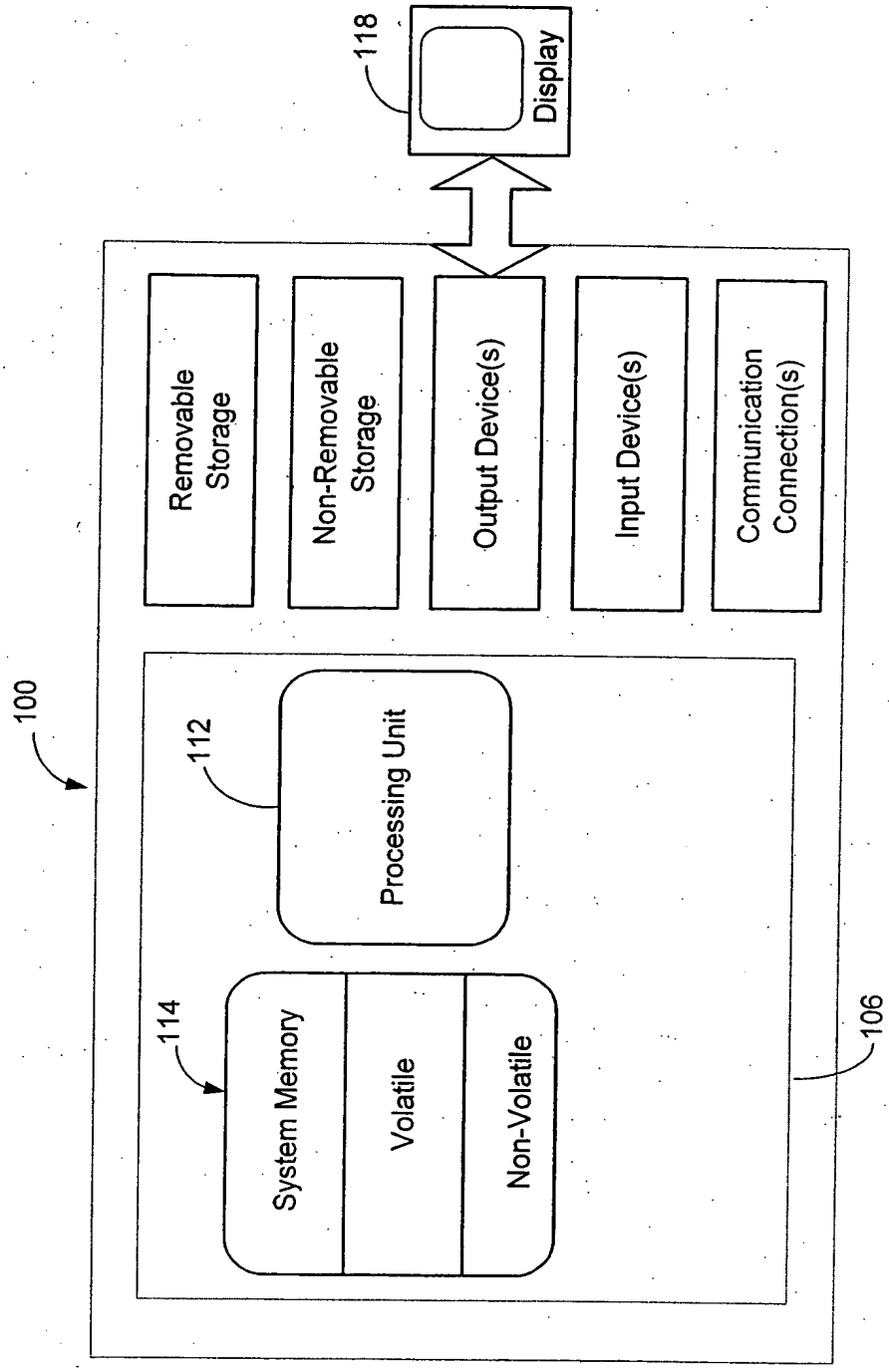

FIG. 2

(Prior Art)

METHOD AND APPARATUS FOR FRAGMENTING AND REASSEMBLING INTERNET KEY EXCHANGE DATA PACKETS
Applicant: Swander et al.
Serial No.: 10/056,889
Docket No.: M1103.70145US00
Figure 3
ANNOTATED SHEET SHOWING CHANGES

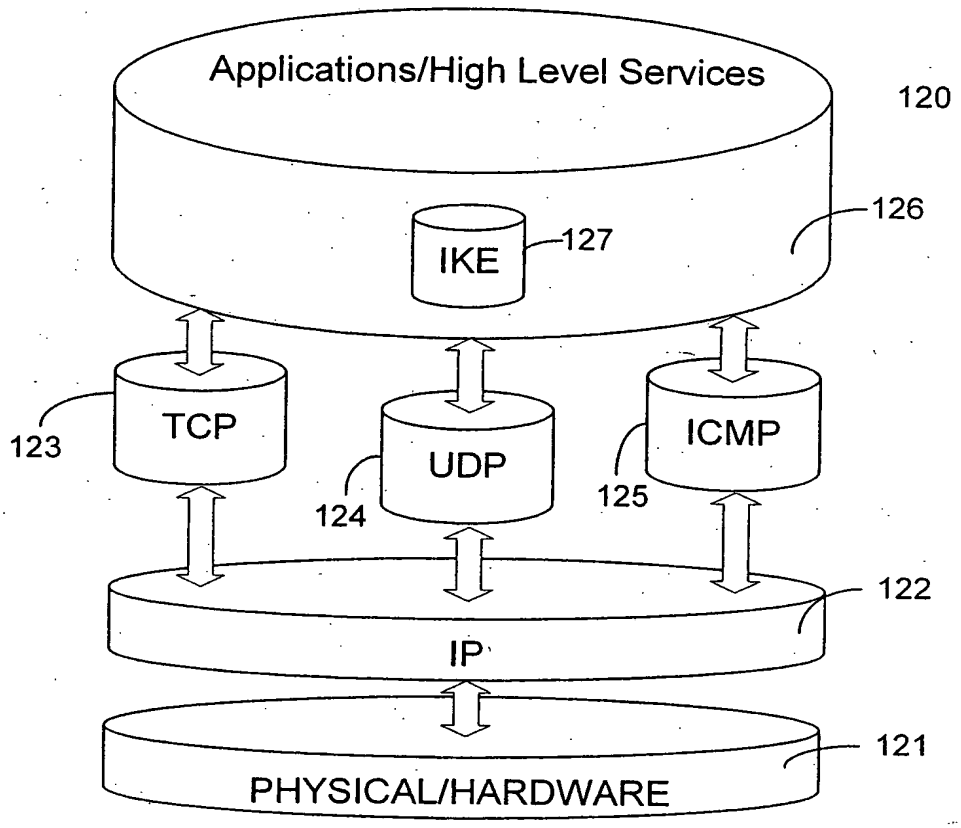

FIG. 3 (Prior Art)

METHOD AND APPARATUS FOR FRAGMENTING AND REASSEMBLING INTERNET KEY EXCHANGE DATA PACKETS
Applicant: Swander et al.
Serial No.: 10/056,889
Docket No.: M1103.70145US00
Figure 4
ANNOTATED SHEET SHOWING CHANGES

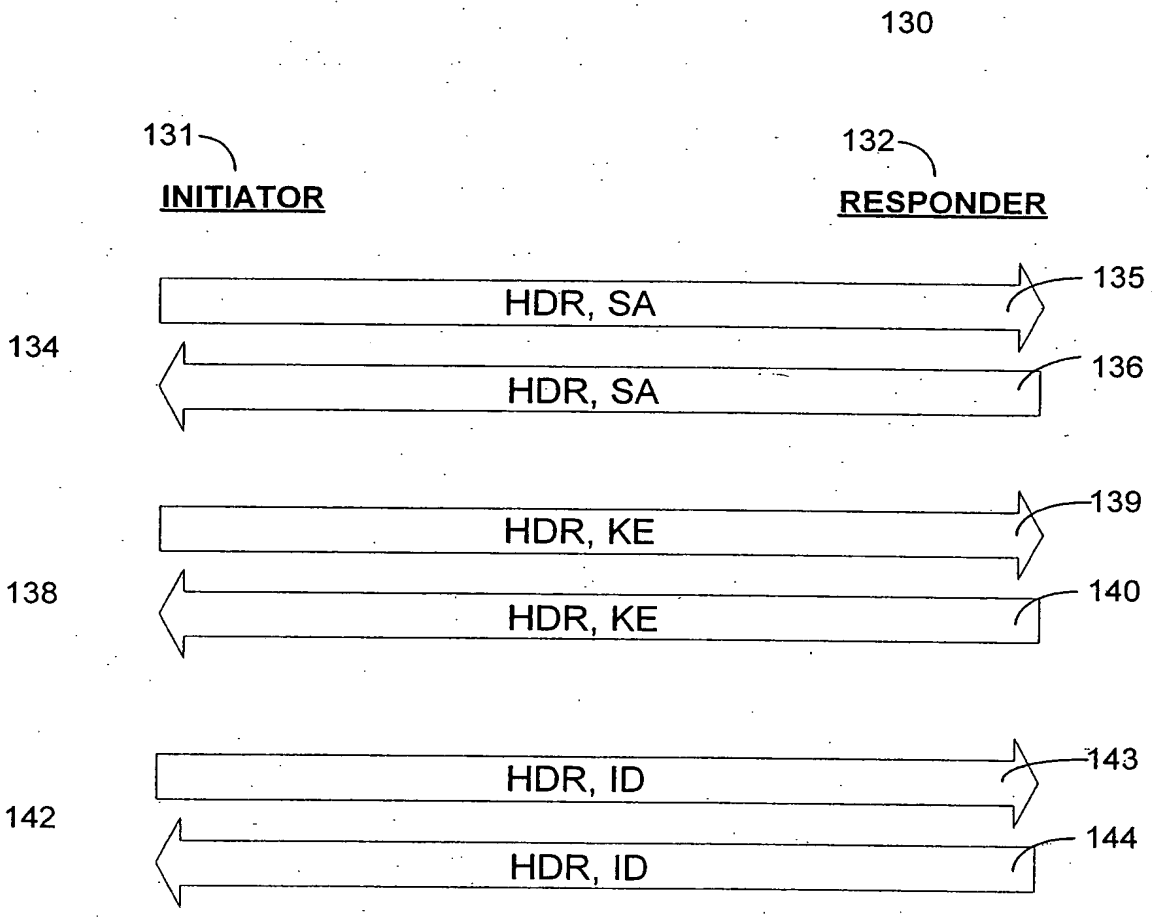

FIG. 4 (Prior Art)